A New Public Key Cryptosystem Based on the Cubic Pell Curve

Michel Seck[1] and Abderrahmane Nitaj[2]

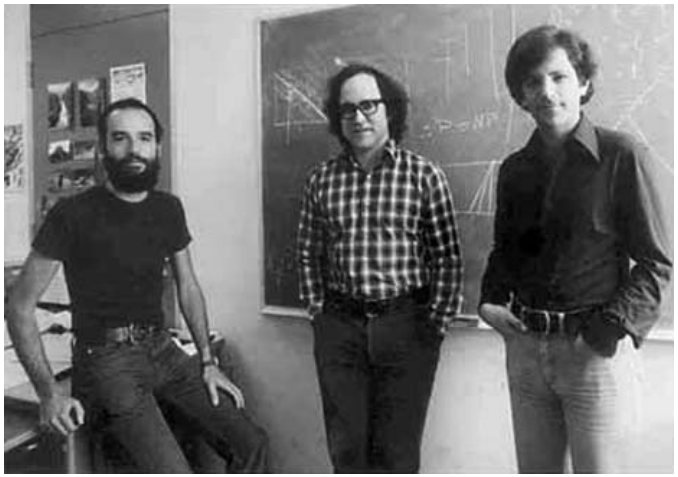
1 Ecole Polytechnique de Thies, LTISI, Senegal
2 LMNO, Université de Caen Normandie, France

NUTMIC 2024 Szczeecin, Poland, June 26, 2024,

Contents

Contents

The RSA Cryptosystem



- Invented in 1978 by Rivest, Shamir and Adleman.
- The most widely used asymmetric cryptosystem.
- Many applications such as encryption and digital signatures.

RSA: The hard problems

The equations

The modulus: $N = pq$,
The key equation: $ed - k\phi(N) = 1$,
The RSA problem: $c \equiv m^e \pmod{N}$.

The Integer Factorization Problem

Let $N = pq$ be an RSA modulus with unknown factorization. Find p and q.

The Key Equation Problem

Given $N = pq$ and e satisfying $ed - k(p-1)(q-1) = 1$. Find d.

The RSA Problem

Given $N = pq$, e and c. Find an integer $m \in \mathbb{Z}_N^*$ such that

$$m^e \equiv c \pmod{N}.$$

Some variants of the RSA Cryptosystem

1. KMOV: Koyama, Maurer, Okamoto, Vanstone, 1991:
   - Modulus $N = pq$.
   - Based on the public elliptic curve: $y^2 = x^3 + b$.
   - Key equation $ed - k\,(p+1)\,(q+1) = 1$.
2. Demytko, 1993:
   - Modulus $N = pq$.
   - Based on the public elliptic curve: $y^2 = x^3 + ax + b$.
   - Key equation $ed - k\,(p+1\pm t_p)\,(q+1\pm t_q) = 1$.
3. Murru and Saettone, 2018:
   - Modulus $N = pq$.
   - Based on the public cubic Pell curve: $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$.
   - Key equation $ed - k\left(p^2+p+1\right)\left(q^2+q+1\right) = 1$.

Contents

The cubic Pell curve

1. Let $\mathbb{F}$ be a field and let $a \in \mathbb{F}$. Define the quotient ring $R_a = \mathbb{F}[t]/(t^3 - a)$.
2. An element $w \in R_a$ can be written as $w = x + yt + zt^2$ for some $(x, y, z) \in \mathbb{F}^3$.
3. Let $w_1 = x_1 + y_1 t + z_1 t^2$ and $w_2 = x_2 + y_2 t + z_2 t^2$ be two elements of R_a. The sum $w_1 \oplus w_2$ is defined by

$$\begin{aligned} w_1 \oplus w_2 = &[x_1x_2 + a(y_2z_1 + y_1z_2)] \\ &+ [x_2y_1 + x_1y_2 + az_1z_2]t + [y_1y_2 + x_2z_1 + x_1z_2]t^2. \end{aligned}$$

4. The norm of $w = x + yt + zt^2$ is given by $N_a(w) = x^3 + ay^3 + a^2z^3 - 3axyz$.
5. The cubic Pell curve over $\mathbb{F}$

$$P_a^3 = \left\{(x, y, z) \in \mathbb{F}^3 : x^3 + ay^3 + a^2z^3 - 3axyz = 1\right\}.$$

The cubic Pell curve

1. Let $N = p^r q^s$ be a multiprime RSA modulus.
2. Consider the cubic Pell curve

$$\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}.$$

3. The cardinality of $\mathcal{PC}_a(p^r)$ is

$$|\mathcal{PC}_a(p^r)| = \begin{cases} p^{2(r-1)}(p^2+p+1) & \text{if } a \text{ is a cubic non residue modulo } p, \\ p^{2(r-1)}(p-1)^2 & \text{if } a \text{ is a cubic residue modulo } p. \end{cases}$$

4. The cardinality of $\mathcal{PC}_a(N)$ is

$$|\mathcal{PC}_a(N)| = |\mathcal{PC}_a(p^r)||\mathcal{PC}_a(q^s)|.$$

The cubic Pell curve

1. For a positive integer n, we define the scalar multiplication of a point $(x, y, z) \in \mathcal{PC}_a$ by n as follows

$$n \otimes (x, y, z) = (x, y, z) \oplus \cdots \oplus (x, y, z) \quad (n \text{ times}).$$

2. For any positive integer k, and any solution $(x, y, z) \in \mathcal{PC}_a(N)$, we have

$$(1 + k|\mathcal{PC}_a(N)|) \otimes (x, y, z) = (x, y, z).$$

3. Depending on a, we have $|\mathcal{PC}_a(N)| = \psi_i(N)$ for $i = 1, 2, 3, 4$ with

$$\begin{aligned}
\psi_1(N) &= p^{2(r-1)} q^{2(s-1)} \left(p^2 + p + 1\right) \left(q^2 + q + 1\right), \\
\psi_2(N) &= p^{2(r-1)} q^{2(s-1)} (p-1)^2 (q-1)^2, \\
\psi_3(N) &= p^{2(r-1)} q^{2(s-1)} \left(p^2 + p + 1\right) (q-1)^2, \\
\psi_4(N) &= p^{2(r-1)} q^{2(s-1)} (p-1)^2 \left(q^2 + q + 1\right).
\end{aligned} \tag{1}$$

Contents

Key Generation

Input: A security parameter λ, and two small positive integers r and s.
Output: A public key pk and a private key sk.

1. Choose a prime number p of λ bit size with $p \equiv 1 \pmod 3$.
2. Choose a prime number q of λ bit size with $q \equiv 1 \pmod 3$.
3. Compute $N = p^r q^s$.
4. For $i = 1, 2, 3, 4$, compute $\psi_i(N)$ using (1).
5. Choose an integer $e \in \mathbb{Z}/N\mathbb{Z}$ such that

$$\gcd\left(e, pq\left(p^2+p+1\right)\left(q^2+q+1\right)(p-1)(q-1)\right) = 1.$$

6. For $i = 1, 2, 3, 4$, compute $d_i \equiv e^{-1} \pmod{\psi_i(N)}$.
7. The public key is $pk = (N, e)$.
8. The private key is $sk = (p, q, d_1, d_2, d_3, d_4)$.
9. Return the keypair (pk, sk).

Encryption

Input: A message $M = (x_M, y_M) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ and a public key $pk = (N, e)$.
Output: The ciphertext of M.

1. Compute $a \equiv \frac{1-x_M^3}{y_M^3} \pmod{N}$.
2. Compute $(x_C, y_C, z_C) = e \otimes (x_M, y_M, 0)$ on the cubic Pell curve with the equation

$$\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}.$$

3. Return the ciphertext (x_C, y_C, z_C).

Decryption

Input: A ciphertext (x_C, y_C, z_C) and a private key sk.
Output: The decryption of (x_C, y_C, z_C).

1. Find the solutions $x = a_{p,1}$ and $x = a_{p,2}$ of the equation
$$x_C^3 + xy_C^3 + x^2 z_C^3 - 3xx_C y_C z_C \equiv 1 \pmod{p^r}.$$
2. Find the solutions $y = a_{q,1}$ and $y = a_{q,2}$ of the equation
$$x_C^3 + yy_C^3 + y^2 z_C^3 - 3yx_C y_C z_C \equiv 1 \pmod{q^s}.$$
3. Use the Chinese Remainder Theorem to compute $a_i \in \mathbb{Z}/N\mathbb{Z}$, $i = 1, 2, 3, 4$ such that
$$x_C^3 + a_i y_C^3 + a_i^2 z_C^3 - 3a_i x_C y_C z_C \equiv 1 \pmod{N}.$$
4. For $i = 1, 2, 3, 4$, choose d_i following a_i.
5. Compute $M_i = (x_i, y_i, z_i) = d_i \otimes (x_C, y_C, z_C)$ on the cubic Pell curve
$$\mathcal{PC}_{a_i}(N) : x^3 + a_i y^3 + a_i^2 z^3 - 3a_i xyz \equiv 1 \pmod{N}.$$
6. Return the plaintext (x_i, y_i, z_i) for which $z_i = 0$.

Contents

Facts on the security

1. The decryption works perfectly.
2. The non uniqueness of the decryption has probability in the interval $\left(\frac{1}{16N}, \frac{16}{N}\right)$.
3. Resistance against finding the cubic Pell curve: Finding the solutions a of the equation

$$x_C^3 + a y_C^3 + a^2 z_C^3 - 3 a x_C y_C z_C \equiv 1 \pmod{N},$$

   is equivalent to factoring N.
4. Even if a is known, there is no discrete logarithm problem:

$$(x_C, y_C, z_C) = e \otimes (x_M, y_M, 0).$$

   Solving this equation is infeasible.
5. Resistance against the small private exponent attacks: Solving the key equation $ed - k\psi_i(N) = 1$ is infeasible for large d.

Contents

Conclusion

- We presented a study of the cubic Pell curve $\mathcal{PC}_a(N) : x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$ for $N = p^r q^s$.
- We proposed a new scheme using the cubic Pell curve.
- We proved that its security is at least as hard as factoring.

Thank you – Dziękuję – Merci